



TITLE:

# 近似代数その1: 近似多項式の四則演算(数式処理における理論とその応用の研究)

AUTHOR(S):

佐々木, 建昭

---

CITATION:

佐々木, 建昭. 近似代数その1: 近似多項式の四則演算(数式処理における理論とその応用の研究). 数理解析研究所講究録 1995, 920: 115-119

ISSUE DATE:

1995-08

URL:

<http://hdl.handle.net/2433/59712>

RIGHT:

## 12.

# 近似代数その1 – 近似多項式の四則演算

佐々木 建昭 (筑波大数学系)

## 12.1 はじめに

筆者は6年前に近似代数の概念を提唱し [1]、共同研究者とともに近似 GCD [2,3] や近似因数分解 [4,5]、多変数代数方程式の近似べき級数解法 [6,7] などの算法を考案してきた。数値計算や応用分野では近似計算は主流をなす計算法であるが、そこでの近似とは「正確な計算の模擬計算」、すなわち「近似は精度が高いほど良い」というものである。一方、近似代数では、多項式や有理式にノルムを定義し、ノルムが微小な項の不定性の範囲内で代数演算を扱う。したがって、微小項は小さいほどよいというものではなく、「この程度以下」というように、場合に応じて規定されるべきものである。近似演算の対象となる多項式を近似多項式と呼ぶ。近似多項式の数係数は近似数である必要はなく（もちろん、近似数であってもよいが）、ノルムが微小な項の不定性を許容するという意味である。

微小項の不定性を導入した場合、通常の代数演算の算法を少し修正すれば事足りると思えるが、実はそうではない。たとえば、従来の因数分解算法は最終的に  $\mathbb{Z}_p$  上の因数分解に帰着されるから、係数部に  $10^{-14}$  程度の誤差が入り込む（浮動小数の計算がそうである）だけで算法は破綻してしまう。この例が端的に示すように、近似代数では従来の代数がそのままでは通用せず、基礎から作り上げていかねばならない。本稿では、第一歩として、近似多項式の四則演算を議論する。

## 12.2 多項式のノルムと $O$ 記号

多項式  $P(x)$  の係数の絶対値のなかで最大のものを  $P$  のノルムと定義し、 $\|P\|$  と表す。

我々は近似代数で、近似の精度として  $10^{-2}$  と  $10^{-4}$  が区別できるような詳細な議論をしたいが、それには積  $G \cdot H$  のノルムの大きさをかなり精度よく評価することが必要である。数の大きさのオーダーを表す記号として、Landau の  $O$  記号がよく使われるが、それは極限值として  $0$ , 有限値,  $\infty$  の3値をとるものと定められているので、近似代数の議論には全く使えない。さて、多項式  $G$  と  $H$  の積を  $F$  とするとき、比  $r = \|F\|/(\|G\| \cdot \|H\|)$  は  $F$  と  $G, H$  によって種々の値をとる。例外的に  $r \ll 1$  となることはあるが、 $r \gg 1$  となることはなく、多くの場合に  $r$  は  $1$  の周りに分布する。 $r \ll 1$  となる場合、積  $G \cdot H$  において組織的桁落ち (systematic cancellation) が生じたという。 $r$  の上限を  $G$  と  $H$  に関わらない形で決めることはできるが、それは一般に近似代数には大きすぎて使えない。また、 $r$  の値を一般の場合に精度よく決めるのは理論的に極めて難しい。そこで、多くの場合に  $r$  の値が  $1$  の周りに分布することに注目して、 $\|G \cdot H\|$  の  $\|G\| \cdot \|H\|$  からのずれを  $r$  の分布の分散で平均的に評価することにする。こうすれば、小さい確率で評価値が狂うことはあっても、平均的には程良い評価値が得られる。

以下では、積  $G \cdot H$  において組織的桁落ちが生じない場合に対して、積のノルム  $\|G \cdot H\|$  はノルムの積  $\|G\| \cdot \|H\|$  と同じ程度の大きさであるとし、それを  $O$  記号で  $\|G \cdot H\| = O(\|G\| \cdot \|H\|)$  と表すことにする。組織的桁落ちを考慮すると、一般には  $\|G \cdot H\| \leq O(\|G\| \cdot \|H\|)$  となる。上述したように、 $O$  記号は比  $r$  の分布の分散と解釈するから、 $G$  と  $H$  の項数に依存することになる。このように  $O$  記号を使うことにより、以下の議論は極めて簡素なものとなる。

## 12.3 近似の精度… acc 記号

多項式  $F$  の数係数が誤差を含み、誤差の上限が  $\varepsilon \ll 1$  であるとき、 $F$  の精度は  $\varepsilon$  であるという。

多項式  $F$  と  $G$  が  $\|F - G\| \leq \varepsilon$  を満たすとき、 $F$  と  $G$  は精度  $\varepsilon$  で等しいといい、次のように表す。

$$\|F - G\| \leq \varepsilon \ll 1 \iff F = G \text{ (acc } \varepsilon)$$

多項式  $F_1, \dots, F_r$  に代数演算  $\text{Op}$  を施し、その結果が精度  $\varepsilon$  で  $G$  に等しいとき、近似演算  $\text{Op}$  は精度  $\varepsilon$  で  $G$  になるといい、次のように表す。

$$\text{Op}(F_1, \dots, F_r) = G \text{ (acc } \varepsilon)$$

## 12.4 従来の除算算法の破綻

多項式  $G$  と  $H$  の精度がそれぞれ  $\varepsilon_G$  と  $\varepsilon_H$  のとき、和  $G + H$  の精度は  $\max\{\varepsilon_G, \varepsilon_H\}$  となり、

積  $G \times H$  の精度は  $\max\{\|G\|\varepsilon_H, \|H\|\varepsilon_G\}$  となる。和と積の演算は従来の算法で行なえばよい。

ところが、従来の除算算法は近似多項式に対しては破綻する場合がある。たとえば、除多項式  $G$  はノルムが1で主係数が小さく、全ての係数に  $O(\varepsilon)$  の誤差が含まれているとしよう。 $G$  の主係数を  $\text{lc}(G) = \eta \ll 1$  とすれば、主係数の精度は相対的に  $O(\varepsilon/\eta)$  しかない。 $F/G$  に対する従来の除算算法は  $G$  の主係数で  $F$  の高次項を割って消去していくものゆえ、 $\text{lc}(G)$  の精度が不足している場合、結果はたちまち誤差だらけとなる。さらに、 $F = GH \pmod{\varepsilon}$  で、 $\varepsilon < |\text{lc}(G)|, |\text{lc}(H)| \ll 1$ ,  $|\text{lc}(G)| \cdot |\text{lc}(H)| = 0 \pmod{\varepsilon}$  の場合、 $\deg(F) < \deg(G) + \deg(H)$  となってしまう…これを次数低下 (degree-decreasing) と呼ぶ。このような場合、従来の除算算法は全く破綻する。

## 12.5 キャンセル数 (cancel number)

数ベクトル  $\mathbf{u} = (u_1, \dots, u_n)$  に対し、ノルム  $\|\mathbf{u}\|$  を次式で定義する。

$$\|\mathbf{u}\| \stackrel{\text{def}}{=} \max\{|u_1|, \dots, |u_n|\}$$

$n$  次元の数ベクトル  $\mathbf{u}_1, \dots, \mathbf{u}_m$ 、ただし  $m \leq n$ 、が数  $c_1, \dots, c_m$  に対し次式を満たすとする。

$$\begin{cases} c_1 \mathbf{u}_1 + \dots + c_m \mathbf{u}_m = (0, \dots, 0) \pmod{\varepsilon}, \\ \max\{|c_1|, \dots, |c_m|\} = 1 / \max\{\|\mathbf{u}_1\|, \dots, \|\mathbf{u}_m\|\}. \end{cases}$$

上式を満たす  $\varepsilon$  のうち、値が最小のものを  $\mathbf{u}_1, \dots, \mathbf{u}_m$  のキャンセル数 (cancel number) と名付け、 $\text{canc}(\mathbf{u}_1, \dots, \mathbf{u}_m)$  と表す。上式は近似線形従属関係である。実際、 $\mathbf{u}_1, \dots, \mathbf{u}_m$  が線形独立な場合、上式が  $\varepsilon = 0$  に対して成立することはないが、 $\mathbf{u}_1, \dots, \mathbf{u}_m$  が微小項を除いて線形従属である場合、その微小項の精度で近似的に線形従属関係が成立する。キャンセル数については次の定理が成立する。

**定理 12.5.1.**  $m \leq n$  とし、 $U$  を  $n$  次元の数ベクトル  $\mathbf{u}_1, \dots, \mathbf{u}_m$  を行とする  $m \times n$  の数値行列とする。 $U$  に対し完全ピボットイング Gauss 消去法により列消去を行なった結果を  $U'$  とすると、

$$U' = \begin{pmatrix} u'_{11} & u'_{12} & \cdots & \cdots & \cdots & u'_{1n} \\ & u'_{22} & u'_{23} & \cdots & \cdots & u'_{2n} \\ & & \ddots & \ddots & \vdots & \vdots \\ 0 & & & u'_{mm} & \cdots & u'_{mn} \end{pmatrix}$$

と表される。このとき  $\text{canc}(\mathbf{u}_1, \dots, \mathbf{u}_m)$  は次式で与えられる。

$$\text{canc}(\mathbf{u}_1, \dots, \mathbf{u}_m) = \frac{O(\|m\text{th row of } U'\|)}{\max\{\|\mathbf{u}_1\|, \dots, \|\mathbf{u}_m\|\}}. \quad \square$$

## 12.6 近似多項式の除算算法

多項式  $F, G, H$  の間には  $F = GH$  ( $\text{acc } \varepsilon$ ),  $\varepsilon \ll 1$  なる関係が成立するとし、 $F$  と  $G$  を与えて商  $H$  を計算することを考える。 $F, G, H$  を以下のように表す。

$$\begin{cases} F(x) = f_l x^l + f_{l-1} x^{l-1} + \cdots + f_0, \\ G(x) = g_m x^m + g_{m-1} x^{m-1} + \cdots + g_0, \\ H(x) = h_n x^n + h_{n-1} x^{n-1} + \cdots + h_0. \end{cases}$$

本稿では簡単のため、 $F, G, H$  は 1 変数多項式で、 $\deg(F) = \deg(G) + \deg(H)$  のとき（すなわち次数低下が生じないとき）のみを扱うが、この制限は本質的なものではない。

$n+1$  個の  $l$  次元数ベクトル  $\mathbf{g}_n, \dots, \mathbf{g}_0$  を次のように定める。

$$\begin{cases} \mathbf{g}_n &= (g_m, \dots, g_0, 0, 0, \dots, 0) \\ \mathbf{g}_{n-1} &= (0, g_m, \dots, g_0, 0, \dots, 0) \\ &\vdots \\ \mathbf{g}_0 &= (0, 0, \dots, 0, g_m, \dots, g_0) \end{cases}$$

$\mathbf{f} = (f_l, f_{l-1}, \dots, f_0)$  とおくと、関係式  $F = GH$  ( $\text{acc } \varepsilon$ ) は次のように表せる。

$$\mathbf{f} - h_n \mathbf{g}_n - \cdots - h_0 \mathbf{g}_0 = (0, 0, \dots, 0) \quad (\text{acc } \varepsilon)$$

これは  $l$  次元ベクトル  $\mathbf{f}, \mathbf{g}_n, \dots, \mathbf{g}_0$  に対する近似線形従属関係であり、次の定理が成立する。

**定理 12.6.1.** 関係式  $F = GH$  ( $\text{acc } \varepsilon$ ) において、 $\|G\| = 1$  として  $G$  を固定した場合、 $H$  の不定性  $\Delta H$  は  $\|\Delta H\| \leq \varepsilon / \text{canc}(\mathbf{g}_n, \dots, \mathbf{g}_0)$  を満たす。 $(H$  の不定性  $\Delta H$  とは  $F = GH = G \cdot (H + \Delta H)$  ( $\text{acc } \varepsilon$ ) を満たすものである。)  $\square$

**定理 12.6.2.**  $n+2$  個の  $l$  次元数ベクトル  $\mathbf{f}, \mathbf{g}_n, \dots, \mathbf{g}_0$  を行とする  $(n+2) \times l$  行列を  $U$  とする： $U = (\mathbf{f}, \mathbf{g}_n, \dots, \mathbf{g}_0)^T$ 。  $U$  の第 2 行以下（すなわち  $\mathbf{g}_n, \dots, \mathbf{g}_0$ ）を使い、完全ピボットイング Gauss 消去法により  $U$  の列消去を行なえば、 $F = GH$  ( $\text{acc } \varepsilon$ ) を満たす  $H$  を計算できる。  $\square$

## 12.7 おわりに

上記の定理の証明は論文 [8] を参照されたい。同論文は、1 変数のみならず多変数多項式の除算も扱い、また次数低下が生じる場合の算法も与えている。さらに、剰余のある除算  $F = GH + R$  ( $\text{acc } \varepsilon$ ) も扱っている。この場合も、商と剰余の不定性はキャンセル数で規定できる。

除算における不定性のみならず、因数分解や GCD などの代数演算においても、因子の不定性の上限や演算の最小精度が問題になるが、それらもキャンセル数で規定できることを論文 [9] は示している。

## 参考文献

- [1] 佐々木建昭：近似的代数計算、数理研講究録、Vol. 676 (1988), 307–319.
- [2] T. Sasaki and M-T. Noda, Approximate square-free decomposition and root-finding of ill-conditioned algebraic equations. J. Inf. Proces., **12** (1989), 159–168.
- [3] T. Sasaki and M. Sasaki, Analysis of accuracy decreasing in polynomial remainder sequence with floating-point number coefficients. J. Inf. Proces., **12** (1989), 394–403.
- [4] T. Sasaki, M. Suzuki, M. Kolář and M. sasaki, Approximate factorization of multivariate polynomials and absolute irreducibility testing. Japan J. Indus. Appl. Math., **8** (1991), 357–375.
- [5] T. Sasaki, T. Saito and T. Hilano, Analysis of approximate factorization algorithm I. Japan J. Indus. Appl. Math., **9** (1992), 351–368.
- [6] T. Sasaki and F. Kako, Solving multivariate algebraic equation by Hensel construction. Preprint of Univ. Tsukuba and Nara Women's Univ., Jan. 1993, 22 pages (submitted).
- [7] T. Sasaki, T. Kitamoto and F. Kako, Error analysis of approximate power series roots of multivariate algebraic equation. Preprint of Univ. Tsukuba and Nara Women's Univ., March 1994, 30 pages (submitted).
- [8] T. Sasaki, A study of approximate polynomials, I – representation and arithmetic –. Japan J. Indus. Appl. Math., **12** (1995) (in press).
- [9] T. Sasaki, A study of approximate polynomials, II – properties of approximate divisors –. Preprint of Univ. Tsukuba, Dec. 1994.